REMARKS

I. Status of the Application

Claims 1-8 are pending in the application. Although the Office Action Summary indicates that claims 1-8 are allowed, Applicant assumes that this was an inadvertent error based on the stated claims rejections described on pages 2-4 of the Office Action. Accordingly, Applicant responds as though claim 1-8 stand rejected under 35 U.S.C. § 102. In response to the rejections, claims 1, 3 and 5-8 are amended herein. Support for the amendments can be found throughout the specification, more specifically, on pages 36-37 of the specification. The amendment to claim 8 is not a substantive amendment and more clearly defines the claimed subject matter in light of the amendment to claim 1. Thus, claims 1-8 remain pending in this application.

II. Claim Rejections under 35 U.S.C. § 102

As shown on pages 2-4 of the Office Action, claims 1-8 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,907,618 issued to Gennaro et al. This rejection is respectfully overcome, as Gennaro et al. fails to disclose all of the features recite in independent claim 1, as amended, and as set forth below.

For example, amended claim 1 recites a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of generating a session key based on a random number, encrypting the original document with the session key to create an encrypted document, generating a proxy key based on a public key corresponding to the selected recipient, and transforming the encrypted document with the proxy key to create a transformed document, wherein the random number used in the generation of the session key is privately maintained by the owner of the original document.

As is stated on pages 2 and 3 of the Office Action, the Examiner asserts that Gennaro et al. teach to encrypt an original document with a session key to create an encrypted document, generate a proxy key based on a public key corresponding to a selected recipient, and transforming the encrypted document with a proxy key to create

a transformed message document. However, Applicant disagrees with the Examiner's contentions for at least the following reasons.

Gennaro et al. teach a method an apparatus for verifiably providing key recovery information in a cryptographic system, for example, a key recovery system for recovering a particular session key K. In Gennaro et al.'s system, the sender, receiver, or law enforcement personnel can recover SKR protected keys, such as session key K, using key recovery agents. (Col. 9, ll. 37-50). The SKR protected keys, such as session key K, are disclosed as being data encryption or decryption keys, for example. (Col. 9, ll. 18-30). The session key K is protected by the SKR system, which is a two-phase system. (Col. 9, ll. 50-59). In the first phase, the sender and receiver establish a common random seed from which key-generating keys, or recovery values, are derived. (Col. 9, ll. 64-66). These key-generating keys are not specific to any particular session key K. (Col. 9, ll. 61-64). The sender then uses the key-encrypting keys to "seal" the session key K by multiply encrypting it. (Col. 10, ll. 28-29). After the session key is suitably encrypted, the sender sends each of a data block including the multiply encrypted session key K and a message encrypted with session key K to the receiver. (Col. 10, ll. 54-58, and Col. 11, ll. 4-6). Using key recovery agents, the receiver or law enforcement personnel would be able to decrypt the multiply encrypted session key K and then decrypt the encrypted message using the recovered session key K.

There is no suggestion whatsoever in Gennaro et al. to first encrypt an original document with a session key to create an encrypted document, and then transform the encrypted document with a generated proxy key based on a public key corresponding to a selected recipient to create a transformed document. Moreover, the fundamental teachings of Gennaro et al. require trust between the sender and the receiver, as is exemplified by the fact that a common random seed, which is the basis for all key recovery encryption in Gennaro et al., is commonly shared between the sender and the receiver. (Col. 9, ll. 60 – Col. 10, ll. 11). There is no such requirement in the claimed invention. If fact, as amended, claim 1 recites that the random number used in the generation of the session key is privately maintained by the owner of the original

document. Therefore, Gennaro et al. fails to teach each and every element of claim 1.

Therefore, Applicant believes that independent claim 1, as amended, is not anticipated by Gennaro et al. under 35 U.S.C. § 102, and respectfully requests that the rejection of independent claim 1 under 35 U.S.C. § 102 be withdrawn. Furthermore, by virtue of their dependency on allowable claim 1, Applicant respectfully requests that the rejection of claims 2-8 under 35 U.S.C. § 102 be withdrawn as well. Accordingly, Applicant requests that claims 1-8 be placed in immediate condition for allowance.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, the Examiner is invited to call the undersigned to expedite the prosecution and work out any such issue by telephone or via the to be scheduled personal interview.

Respectfully submitted,

Carlos R. Villamar
Registration Number 43,224

Date: **January 5, 2005**

NIXON PEABODY LLP
401 9th Street, NW
Washington, DC 20004
(202) 585-8000